Università degli Studi di Padova

Department of Information Engineering

Master Thesis in Telecommunication Engineering

GNSS multiantenna receivers under multiantenna spoofing attacks

Supervisor
Laurenti Nicola
Università degli Studi di Padova

Co-supervisor
Silvia Ceccato
Università degli Studi di Padova

Master Candidate
Andrea Pittaro

15 April 2019

Università degli Studi di Padova

Department of Information Engineering

Master Thesis in Telecommunication Engineering

GNSS multiantenna receivers under multiantenna spoofing attacks

Supervisor
Laurenti Nicola
Università degli Studi di Padova

Co-supervisor
Silvia Ceccato
Università degli Studi di Padova

Master Candidate
Andrea Pittaro

15 April 2019

To my Mom and Dad, who always have had my back.

Abstract

The problem of an attack on the Global Navigation Satellite System (GNSS) signal began to be investigated in the early 2000s. [1] However, this was brought to the general public's attention after the release of the game Pokemon Go, when it was shown that the average person could spoof a signal with relatively cheap equipment. During the mid-2010s, both review papers about this topic [1, 2, 3, 4, 5] and new research on attacks and countermeasures have been produced. [6, 7, 8, 9] Although different attacks have been proposed, no one, to the best of the author's knowledge considered the possibility that the attacker could have a multiantenna system, so that he could exploit the Multiple Input Multiple Output (MIMO) capabilities to attack the GNSS signal. This thesis aims to show a possible technique where the attacker could spoof the signal at the receiver, inducing the victim to follow the spoofed path. At the end, some defenses to counteract this attack will be suggested.

Sommario

Il problema delle minacce ai segnali GNSS iniziò ad essere indagato nei primi anni 2000 [1]. Tuttavia l'interesse è stato portato alla luce del grande pubblico con il rilascio di Pokemon Go, quando venne mostrato che chiunque potesse falsificare un segnale GPS con dispositivi abbastanza economici. Durante la metà degli anni 2010, sono stati prodotti numerosi paper, sia di review [1, 2, 3, 4, 5], che nuove ricerche su possibili attacchi e contromisure. [6, 7, 8, 9]

Nonostante ciò, al meglio delle conoscenze dell'autore, nessuno ha considerato la possibilità che un attaccante possa essere dotato di un array di antenne, tale da permettergli di sfruttare le tecniche di MIMO. Questa tesi ha come obiettivo presentare uno scenario in cui l'attaccante riesce a effettuare lo spoofing del segnale satellitare, inducendo il ricevitore a credere che la sua posizione sia quella voluta dall'attaccante. Nelle conclusioni verranno presentate alcune possibili tecniche di difesa per limitare le possibilità di questo attacco.

Contents

List of figures

List of tables

Acronyms

BeiDou BeiDou Navigation Satellite System. xiii, 1, 16, 20, 21

BOC Binary Offset Carrier. 14

BPSK Binary Phase Shifting Key. 11

DoA Direction of Arrival. xi, 27, 30, 31, 33–35

FDMA Frequency Division Multiple Access. 13

GALILEO GALILEO. 1, 6, 8, 14, 15, 20

GLONASS GLObalnaya NAvigatsionnaya Sputnikovaya Sistema. 1, 5, 6, 8, 13, 20, 21

GNSS Global Navigation Satellite System. v, vii, xi, xiii, 1, 2, 6, 8, 9, 13, 14, 16, 17, 20, 25, 26, 37

GPS Global Positioning System. 1, 5–7, 11, 20, 21

IF Intermediate frequency. 10

IP Integrity Protection. 15, 19–21, 37

LoS Line of Sight. 6, 27, 28

MIMO Multiple Input Multiple Output. v, 25, 26

MuSiC Multiple Signal Classification. 30

NLoS Non-Line of Sight. 28

NMA Navigation Message Authentication. 20, 21

PRN Pseudo Random Noise. 8

PVT Position, Velocity and Time. 9, 18

SNR Signal-to-Noise Ratio. 26

SV Space Vehicle. 1, 6, 8–10, 13, 14, 18, 22, 27

TESLA Time Efficient Stream Loss-tolerant Authentication. xi, 20, 21

USA United States of America. 5, 6

USSR Union of Soviet Socialist Republics. 5

1 Introduction

To reach from one position to another, many users rely on the American Global Positioning System (GPS) or the Russian GLObalnaya NAvigatsionnaya Sputnikovaya Sistema (GLONASS), to name the two most famous GNSS. Making the position reliable and accurate was initially seen as important only for military operations. Civilians, on the other hand, received a coarser position, given that the calculations they could make from the signals received by each satellite (also known as a Space Vehicle (SV)), were limited by imposed inaccuracies called Selective Availability (SA). On 1 May 2000, U.S. president Bill Clinton[10] removed SA from the civilian usage and the precision of the signal received could reach 1m. In April 2014, another GPS constellation signal began to be transmitted [11]: the L2C allows for even greater precision thanks to better detection of the atmospheric parameters. As will be discussed in the following chapters, the properties of the atmosphere are the key to being able to identify where the receiver is located. Until now, I have only detailed GPS, as it is the most known and the oldest fully-operational system, but in Table 1.1, I will show the main parameters of each system.

Each GNSS system uses a specific frequency band to transmit the navigation data so that the receiver can compute its own position from the delay of the signal. To avoid spoofing attacks, GPS, GLONASS, GALILEO (GALILEO) and BeiDou offer both an open and free to use service, with coarse precision around 10m, and an encrypted signal for military or commercial operations that reaches a position accuracy around the 10cm range. A replication

Table 1.1: Comparison of the GNSSs

Satellite System	GPS	GLONASS	GALILEO	BEIDOU
Frequencies (GHz)	L1: 1.563–1.587 L2: 1.215–1.2396 L5: 1.164–1.189	G1: 1.593 – 1.610 G2: 1.237 – 1.254 G3: 1.189 – 1.214	E1: 1.559 – 1.592 E5a/b: 1.164 – 1.215 E6: 1.260 – 1.300	B1(-2): 1.5611 - 1.5897 B2: 1.20714 B3: 1.26852
Accuracy	5 - 15m	4-7m	1m	10m
Accuracy military or commercial	$\leq$ 0.715 m	0.1 m	0.01 m	1m

attack on the military signal, though, could always be performed with different accuracies on parameters that will be discussed in subsection 2.4.1. Thus, the only thing a receiver can do is try to mitigate the spoofing attack it has been experiencing.

Even though the damage done when attacking an encrypted GNSS signal is much more than when attacking an open signal, the latter has an audience that is much broader and more vulnerable to such an attack. Today, many rely on GNSS services. For example, a research made by Verto Analytics [12] shows that in April 2018, there were around 232.2 million unique users a month (18+ years old, the age information is given by the birth date in the registration process) in the US alone. According the US census website, the population in July 2018 was estimated to be around 327.2M people. This means that more than 70% of Americans use a Map app monthly. Many professional fields rely on satellite navigation to deliver their services, like ATMs, armored trucks, planes, and ships. All of the aforementioned depends heavily on the reliability, accuracy, and trustworthiness of the GNSS signal. The literature analysis showed how legitimate receivers can defend themselves against a spoofer who has one antenna using a linear or planar array of elements. No paper before has hypothesized that the attacker could spoof the signal using an array. This would reduce the capabilities of the legitimate receiver to identify the source of the transmission and limits the likelihood of a successful spoofing attack by ignoring that direction.

This thesis will discuss a possible attack that may mislead the receiver about a GNSS signal without the victim to be able to recognize the legitimate data from the faked. The structure will be as following: Chapter 2 will briefly describe the current state of the GNSS systems, and in Chapter 3 their security. Then, in chapter 4 the proposed attack will be detailed,

focusing on the conceptual and the mathematical principles behind this technique. Finally, in the last part of Chapter 4, I will show some simulation results. The conclusion will then summarize all of the above and will suggest what could be the next steps to improve this attack.

2

The GNSS systems

2.1 History

During the Cold War, both the Union of Soviet Socialist Republics (USSR) and the United States of America (USA) were developing atomic bombs and beginning the Space Race. Keeping an eye on the other superpower was a necessity for both the USA and the USSR, and because of this, they started developing of satellites to be able to position themselves.

When project development on the GPS began in 1951[13], the available system to position a submarine used the Doppler effect of satellites whose positions are known. Acquiring a fixed point with six satellites in orbit required a couple of minutes, but this was not a sufficient system[14]. So in the 1970s, the US government developed an accurate positioning system which was also able to detect nuclear explosions happening around the world [15]. The constellation started to be launched in 1978 and became fully operational in 1993 with different precisions between military and civil navigation signals. The latter, in fact, was degraded with the implementation of a Selective Availability(SA). This prevented anybody other than the military from obtaining a precision signal under 15 meters accuracy.

On the other side, the USSR launched 31 Tsiklon satellites between 1967 and 1978 to accurately position Soviet submarines. [16] To obtain an accurate position, though, the vehicle needed to keep its position fixed for several hours and the tracking was stable only with slow navigation. During the 70s, the USSR developed its navigation system, called GLONASS, which consists of 24 satellites orbiting in the Medium Circular Orbit at 20000km above

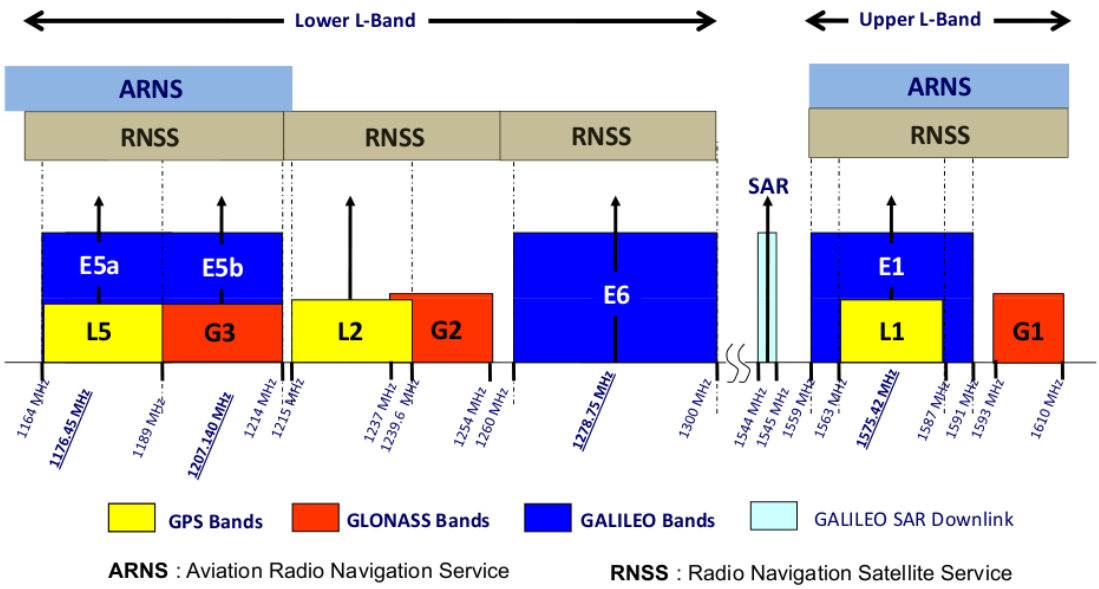


Figure 2.1: A representation of the GNSS bands. Courtesy of gssc.esa.int

Earth's surface. The service they provided was designed to have an accuracy of 65m for civilians, but the actual precision was around 20m. Unlike the GPS, GLONASS didn't implement any SA, so a high precision signal was available to everyone. [16]

Over the years, other countries like India, China, and Japan developed their regional navigation satellite system in order to be independent from the USA or the Russian Union. A new competitor, the European Union (EU), joined the market in February 1999 when the development of GALILEO started. Then, on 28 December 2005, the first satellite, Giove A, was sent to validate the system. The first operational satellite was launched on 22 August 2014 and the constellation should be fully operational by 2020. The EU, then, will be the first entity to provide commercial navigation services to civilians with accuracies on the order of 1cm.

2.2 Signal structure and properties

All GNSS systems are such that a device can receive a Line of Sight (LoS) signal, which is corrupted by the atmosphere then decoded to obtain satellite navigation data and compute the receiver position. All satellites belonging to a system transmit at the same frequency, so to identify the information coming from a specific satellite, the sinusoid is composed with a PRN, an unique identifier of the SV, and the actual navigation data. The composition of

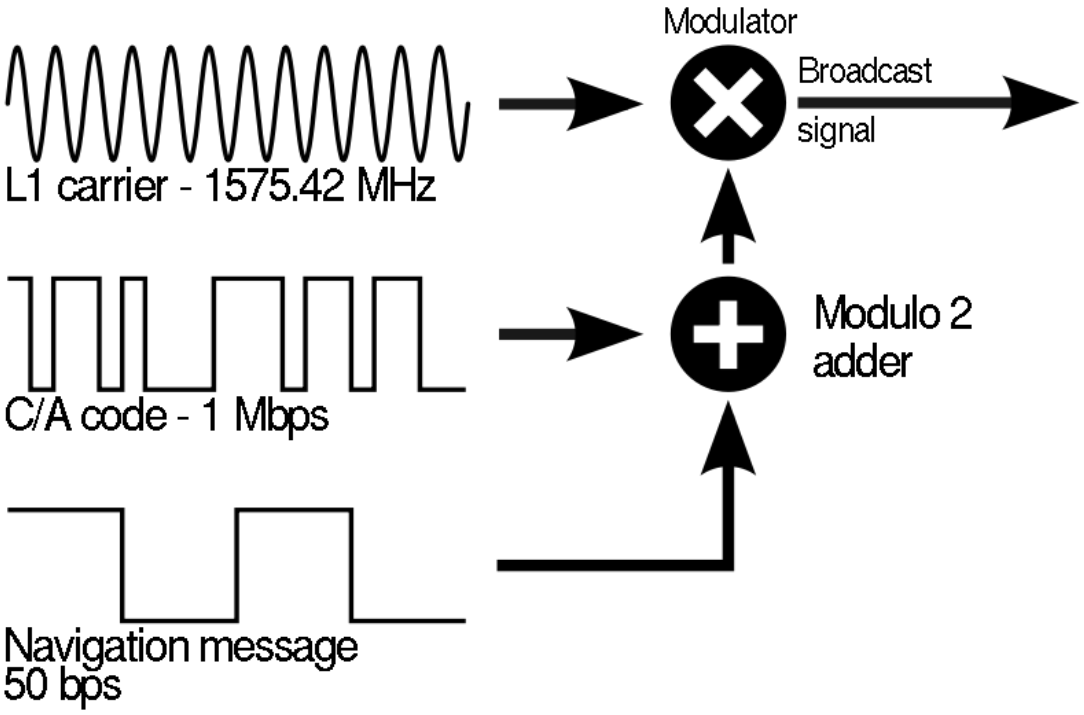


Figure 2.2: The GPS L1 C/A (Coarse Acquisition) signal composition. Source: wikipedia.org

the GPS is illustrated in Figure 2.2. The maximum power of the GPS satellite signal at sea level, for example, is $-158dBW$ which corresponds to $\approx 158.5 \cdot 10^{-18}W$ as shown by [5]. For comparison, in a city center, the LTE (Long Term Evolution) average received power is $-110dBW$, which corresponds to $10pW = 10 \cdot 10^{-12}W$, an increase of more than 5 orders of magnitude. To avoid signal degradation due to the multipath replicas, the signal is right-circularly polarized so that the first reflection becomes left-circularly polarized and is not received by the GNSS antenna. Although the evenly-reflected multipath replicas can be received, the power is low enough to be compared to the noise floor.

As shown in Table 1.1, all four main systems transmit to a common frequency so that one GPS receiver can correctly decode the signals from all other systems as they become operative. This chapter will continue with a section describing the signal's structure and properties, the signal creation, and the position calculation with the correlation analysis, which will be useful for the next chapter. Next chapter will deal with the security of the signal and the anti-spoofing techniques that are currently available. To allow interoperability between the different systems, the open signal, which is publicly available, is transmitted in the same frequency band with one center frequency. To avoid interference that will disrupt the signal,

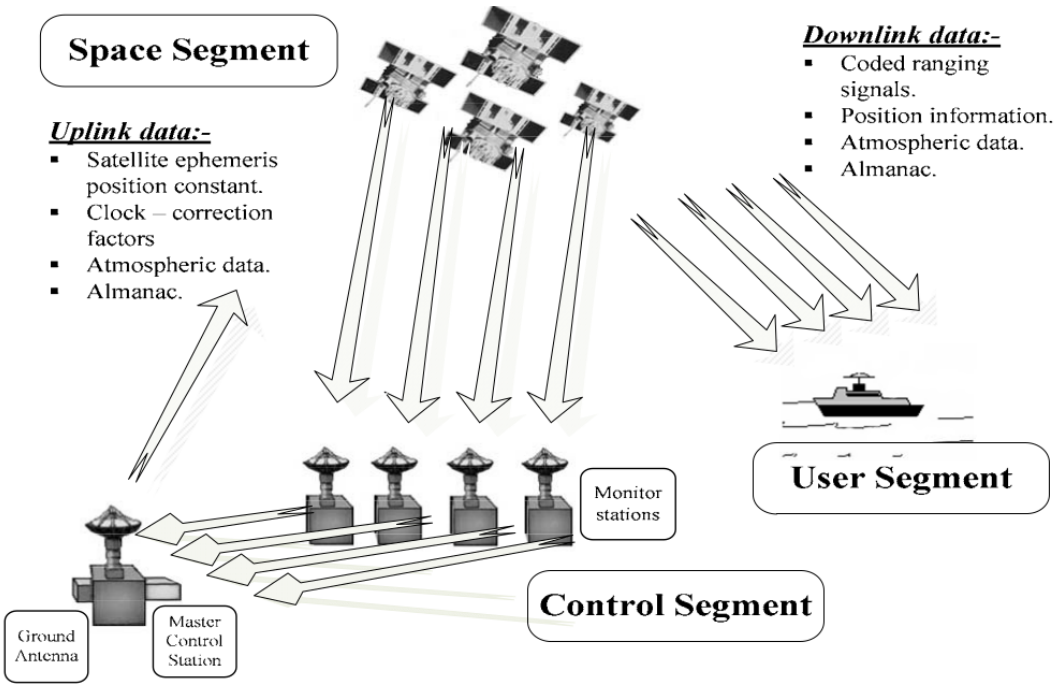


Figure 2.3: How a GNSS system works. The reader can see how the navigation message is sent by the ground center, which monitors the received signal

several Pseudo Random Noises (PRNs) have been created so that the CDMA signal can be retrieved from each satellite. Then, the bits are coded into phase changes, which allows for better decoding capabilities given that the signal is heavily degraded. The SV also needs to transmit information so that each receiver can find its position just by listening to the satellites. In fact, the source of the signal is in an elliptic orbit, between 19130km of GLONASS and 23222km of GALILEO. The properties of the atmosphere change over time and this affects how the signal will propagate and reach the receiver. This means that the satellite must communicate this athmospheric information to the receiver so that the latter can compute its position.

2.3 Signal generation

Ground stations send each satellite its navigation information, which will be transmitted to the receiver daily. NASA website* provides the daily updated information about the satellite parameters for all the GNSSs. The general signal formation process involves the generation

*https://cddis.nasa.gov/Data_and_Derived_Products/GNSS/RINEX_Version_3.html

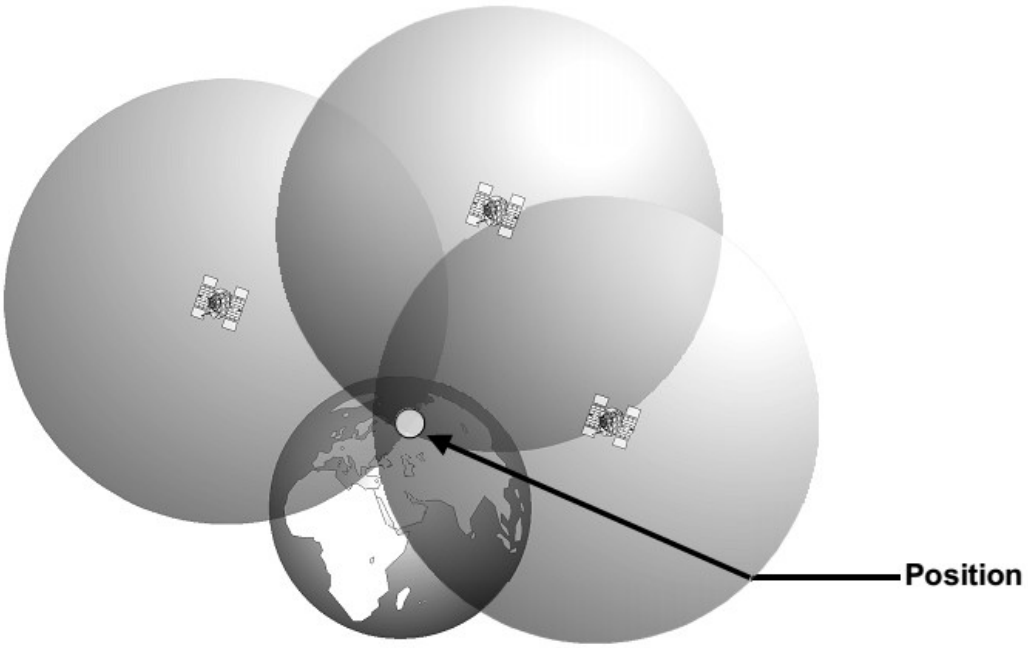


Figure 2.4: How a receiver can calculate its position if it has a clock perfectly synchronized with the satellites one. If this hypothesis is not met, another satellite is required.

of the sinusoid at the center frequency. Then, the signal will go into the convolution process with the PRN code, that has its chip frequency, and the navigation message, that is usually a low-bitrate signal. In Figure 2.2, the signal generation of the main GNSS systems is shown.

2.4 Position calculation

In order to compute the Position, Velocity and Time (PVT) solution, the receiver needs to see at least 4 SVs and needs the full navigation message from them. The first requirement allows the user to receive the position in three dimensions and the time reference, whereas the latter is used to determine the exact position of the satellite in space. For faster position retrieval, the navigation message can be downloaded into the receiver from the BTS if the receiver device has a mobile connection possibility. Otherwise, before being able to have an accurate position, the device needs to wait around 10-15 minutes listening to the GNSS signal. In particular, to compute the position, the device starts a loop in which it executes the following steps [17]:

1. The receiver filters the signals acquired by one or more antennas in the bandwidth of interest, as shown by Table 1.1.

2. The signal is then downconverted to an Intermediate frequency (IF), which is then sampled with an ADC and digitalized.

3. Given the sampled data, the receiver generates the signals for all the satellites. This is possible as the code is unique for each satellite.

4. The sampled received signal is correlated to the local replica of each satellite signal. This leads to finding the peaks of the correlation function and identifying which satellite signals are being received by the device.

5. Knowing the satellites a user sees, the algorithm calculates the propagation delay that occurred, knowing that there are clock offsets both at the receiver side (δ_R), and, in minor part, also at the SV side (δ_S). To do so, it needs at least four satellites. At the same time, the signal is heavily shifted in frequency because of the Doppler effect generated by the satellite moving in space, so the receiver calculates the entity of the frequency shift.
   For the clock offset, given S the satellite and R the receiver, we have:

$$\begin{aligned} D_R^S &= v \cdot \Delta t && \text{The distance formula} \\ & && \text{if speed and delay are known.} \\ D_R^1 &= c \cdot [(t_R - \delta_R) - (t_S - \delta_S)] && \text{The distance formula accounting the offsets} \\ &= c \cdot \Delta t + c \cdot \Delta\delta = \rho + c\Delta\delta && \text{Where } \rho \text{ is the true distance} \end{aligned} \tag{2.1}$$

   In general $\rho = \sqrt{(X_R - X_S)^2 + (Z_R - Z_S)^2 + (Z_R - Z_S)^2}$ with values in the coordinate system.
   For the Doppler shift we have:

$$\begin{aligned} \Delta\phi_R^S + N &= \frac{f}{c} \cdot \rho + f \cdot (\delta_R - \delta_S) \\ \lambda\Phi &= \rho + c\Delta\delta + \lambda N \qquad \text{Rearranging with } \Phi = -\Delta\phi_R^S \end{aligned} \tag{2.2}$$

6. Once the signals are identified, the algorithm either requests the navigation message for each visible satellite from the mobile network base stations, or it enters in the time locked loop and phase locked loop state, where it decodes the full navigation message from each satellite. The latter may require several minutes to be completed. The navigation message from one SV gives information about that satellite's condition, its time offset respect to the reference time, current position, and speed and acceleration of that SV with respect to the coordinates the system uses. More details will be given when dealing with the specific GNSS in section 2.5, section 2.6, and section 2.7.

7. When the messages from all the visible satellites are obtained, the receiver can compute the position and estimate both the troposphere and the ionosphere delay according

to their properties at that time.

2.4.1 Signal correlation

As described in step 4, to compute the position, the receiver needs to isolate the signal from each satellite. This is heavily degraded from the atmosphere, so at first, the analysis finds the signal most correlated with the local replica. From there, the device locks the signal and starts receiving and decoding the navigation message. Once all the data is received, the algorithm knows where the satellite is, and from that moment it can compute the position.

2.5 GPS

The GPS is the oldest operating GNSS system in the world. Launches started on 22 February 1978 with the Block I group and GPS became fully operative for both military and civilian use when Block II was sent on 1 October 1990. This system uses the WGS84 coordinate system [18] to accurately model the Earth. Each satellite transmits its data through a Code Division Multiple Access (CDMA) channel access and the Binary Phase Shifting Key (BPSK) modulation scheme. The advantage of this type of transmission is that the receiver needs only one band to be received, and the code is strong against the attenuation. Each satellite transmits 6 signals per millisecond that are made from a sinusoid at 10.23 MHz and multiplication factors that allows to include the PRN sequence and reach for the final frequencies on where they will be transmitted. A device receiving the L1CA and L2 signals without any mobile connection need 12.5 minutes with the signal in the locked loop before being able to determine its own position. On Table 2.1 there are the characteristics of the signals.

2.5.1 Military applications

Since GPS was created by the United States DoD (Department of Defense), its main application was to provide accurate positioning for military operations of the US government and its allies. While the accuracy for a civilian is around 5 meters, for military applications, it is lower than one meter. There are two military-specific signals: the P and the M code. The first uses a signal orthogonal to the the L1CA, and exploits the aforementioned. In fact, the P-code is a long PRN that is transmitted at a bitrate 10 times higher than the L1CA. To better identify the troposphere and ionosphere delay, the P code is transmitted at the L2C

Signal name	Frequency band (GHz)	Channel access	Modulation	User availability	Navigation message bitrate
L1 C/A	1.57542	CDMA	BPSK(1) (Q)	Open	50 bps NAV
L1 P(Y)	1.57542	CDMA	BPSK(10) (I)	Military	50 bps NAV
L1C	1.57542	CDMA	TMBOC(6,1,1/11)	Open	25bps CNAV
L1M	1.57542		BOC(10,5)	Military	N.A.
L2C (L2CM & L2CL)	1.2276	CDMA	BPSK(1)	Open	25bps (CNAV) 25bps (NAV) 50bps (NAV)
L2 P(Y)	1.2276	CDMA	BPSK(10)	Military	50bps
L2M	1.2276	CDMA	BOC(10,5)	Military	N.A.
L5	1.17645	CDMA	BPSK(10) (I) BPSK(10) (Q)	Open	25bps (CNAV) No NAV

Table 2.1: GPS frequency band

frequency as well. If flagged in the navigation message, the P-code can be modulated with a W code to generate the P(Y) code. This is done to prevent the spoofing capabilities that will be further discussed in section 3.2. The M code [19], however, is still not operative, but is designed to transmit navigation information independently on the civilian signal and allows, when set by ground centers, for the use of directional antennas to hit a spot beam, where power is increased and the BOC(10,5) modulation allows the signal to have less of its spectrum disturbed by the existing CA and P(Y) codes.

2.6 GLONASS

GLONASS is the GNSS system developed by the former USSR and maintained by the Russian Federation. The first satellite was sent to orbit on 12 October 1982 and the constellation became fully operative both for civilian and military use in 1995. GLONASS has its own coordinate system, the PZ-90, which was created after observing the Earth's surface for 20 months in order to better model it.

Five signals are transmitted, four using Frequency Division Multiple Access (FDMA) and one using CDMA. After the fall of the Soviet Union, the satellites weren't replaced and GLONASS stopped working. Then, in 2001, Putin started renovating the satellites and by 2010 full coverage was restored. Today, Russia is developing new satellites to cover more frequencies so that a receiver can better estimate the ionosphere and troposphere error. The new SVs will provide more CDMA signals that will transmit at the same frequency of the other two GNSS.This will allow for the creation of devices that can receive between one and three carrier frequencies of the GNSS spectrum and are able to decode the signals from all four GNSS systems. A summary of the GLONASS system can be found in 2.2.

2.6.1 Military applications

In order to have their own position capabilities, GLONASS was initially developed to provide meter accuracy for the Russian army. The precision code was given to the scientific community to be tested: this means that everyone can receive the high precision code and compute their position with high accuracy. The Russian army, though, reserves the right to change the P-code in the future [20].

Signal name	Frequency band (GHz)	Channel access	Modulation	User availability	Navigation message bitrate
L1 OF	1.602 + n * 0.0005625	FDMA	BPSK(0.511)	Open	50 bps
L1 SF	1.602 + n * 0.0005625	FDMA	BPSK(5.11)	Military	N.A.
L2 OF	1.246 + n*0.0004375	FDMA	BPSK(0.511)	Open	50 bps
L2 SF	1.246 + n*0.0004375	FDMA	BPSK(5.11)	Military	N.A.
L3 OC	1.202025	CDMA	BPSK(4) or BPSK(8)	Open	100bps or 125 bps
L1 OC	1.600995	CDMA	BPSK	Open	100bps

Table 2.2: Glonass Signals

2.7 Galileo

GALILEO is the European GNSS that was meant to offer guaranteed high precision services both to civilian, through the commercial navigation service signal and to governmental or military applications, with the Public Regulated Navigation signal. [21, 22] The first launch was on 21 October 2011 and the constellation will be fully deployed by 2020. The signals were originally designed to be transmitted at the same frequency as GPS, but for security reasons, they were shifted to the frequencies that can be seen in Table 2.3. By doing so, the US and Russia can, in case of an attack, jam all other GNSSs signals except for their own. GALILEO signals are modulated with a Binary Offset Carrier (BOC) scheme and a CDMA channel access. There are 4 frequencies transmitted by each SV that allow to send five types of signals:

Open Access which is publicly available and guarantees precision up to 1m

Commercial Navigation which is the encrypted version of the Open Access and guarantees precision up to 1cm

Signal name	Frequency band (GHz)	Channel access	Modulation	User availability	Navigation message symbols per second
E1 OS	1.57542	CDMA	CBOC(6,1,1/11)	Open	250 sps
E1 PRS	1.57542	CDMA	BOC(15,2.5)	Governmental	N.A.
E6 CS	1.27875	CDMA	BPSK(5)	Commercial	1000 sps
E6 CS	1.27875	CDMA	BPSK(5)	Commercial	0
E6 PRS	1.27875	CDMA	BOC(10,5)	Governmental	N.A.
E5a	1.191795	CDMA	AltBOC(10,5)	Open	50 sps
E5b	1.191795	CDMA	BOC(10,5)	Open	250 sps

Table 2.3: Galileo Signals

Safety of Life is an open service and it's used for situations where it is necessary to guarantee precision and availability.

Public Regulated Navigation an encrypted signal and the only GALILEO signal guaranteed to be always operational to EU countries in case of a crisis.

Search and Rescue the service that locates and retransmits the emergency rescue signals that are deployed if an accident happens. It has the ability to forward the replies sent by the rescue centers to the source of the emergency signal.

2.7.1 Commercial applications

In general, applications for which GALILEO can be used include agriculture, ATMs, aircrafts, and ships, as they need a system that guarantees precision within a centimeter and is not limited by a country if they fear a threat. The signal that will be received by a device enabled for commercial service can be assured that the signal received is legitimate and not spoofed since Integrity Protection (IP) is implemented on the signal using a symmetric cryptographic mechanism.

have the assurance to be the legit one and not the spoofed one, as it is implemented the Integrity Protections (IP) on the signal via a symmetric cryptographic mechanism.

Signal name	Frequency band (GHz)	Channel access	Modulation	User availability	Navigation message bitrate
B1 GSO	1.561098 and 1.589742	CDMA	QPSK(2) (I)	Open	50 bps
B1 N-GSO	1.561098 and 1.589742	CDMA	QPSK(2) (I)	Authorized	500 bps
B1 GSO and B1 N-GSO	1.561098 and 1.589742	CDMA	QPSK(2) (Q)	Authorized	500 bps
B1	1.57542	CDMA	MBOC(6,1,1/11)	Open	50 bps or 100 bps
B2	1.19179	CDMA	AltBOC(15,10)	Open	25 bps or 50 bps
B3	1.26852	CDMA	QPSK(10)	Authorized	500bps

Table 2.4: BeiDou Signals

2.8 BeiDou

The Chinese satellite constellation, BeiDou, was only meant to provide regional positioning over China from 30 October 2000 until April 2007, when the first satellite from the BeiDou-2 system was launched and started providing positioning service to Eastern Asia. With BeiDou-3, China is creating the fourth GNSS system. The coordinate system is called GCJ-02, and it's similar to the WGS84 with the exception that it adds pseudo random offsets to the coordinates given to unauthorized users in order to avoid threats over China. Only Chinese-government approved devices can decode the coordinate system and return the position with an accuracy of 10 meters for open signal and 10 cm for military purposes. A summary table is provided in Table 2.4.

3

Threats, security services and countermeasures

As written in the introduction, many of our devices, systems, infrastructures, and, ultimately, users rely on the accuracy of the GNSS systems, so it is undoubtedly clear that security measures are mandatory. When Pokemon Go became popular, it was obvious that commercial tools to fake the position were available to everyone and that spoofing devices did not cost much [23].

3.1 Threats to GNSS

There are two main threats to the GNSS: jamming, where signal is completely disrupted, and spoofing, in which the legitimate signal is substituted with a signal generated by an attacker. The latter threat is particularly devious, since the victim may be unaware of their condition. Moreover, a spoofed signal may contain a modified version of the navigation message carried in the GNSS signal. The outcome of this attack is that the receiver will download the navigation message only once, then compute accurate predictions for the following couple of hours. The predictions, though, will also be a victim of the attack, so with less than 20 minutes of attack, the victim will remain so for hours.

For the rest of the chapter, I will not deal with the jamming attack. Instead, I will focus and expand the spoofing threats, as the proposed attack I will present in the following chapter

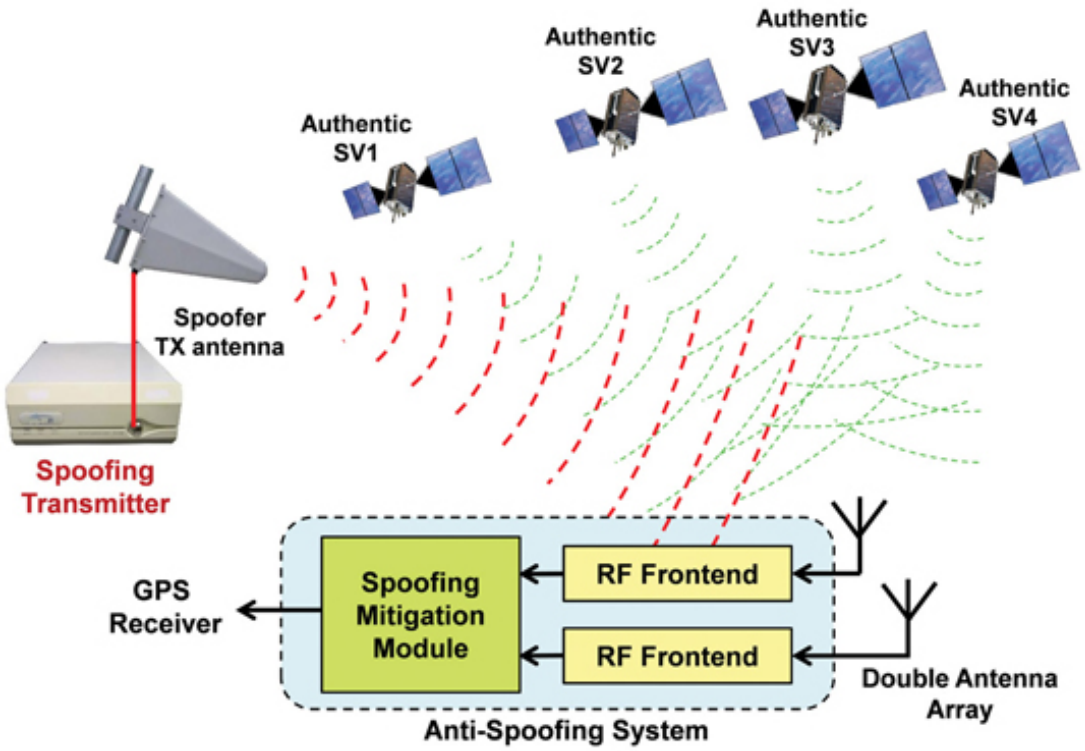


Figure 3.1: An example of a spoofing scenario. Credits to gpsworld.com

will be useful with the latter type.

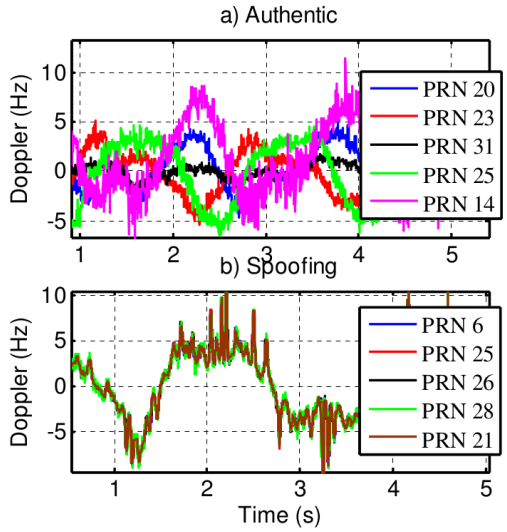
3.2 Spoofing threats

Open access signals do not implement any message authentication or integrity protection over the signal sent by the satellite. This means that anyone who has a GNSS signal generator can spoof a receiver with its own signal. Without an authenticated signal, an attacker could do a reply attack where it can just separate the signals coming from the different SV and retransmit them to the victim with the delay the attacker wants so that the receiver will compute the PVT solution the attacker wishes to spoof.

To date, the defenses against forged signals depends on the system: there have been numerous reports of civilian equipment being spoofed and redirected while using the GPS. Literature has shown that many countermeasures can be adopted when the signal properties are known [24, 5]. Main security measures take into account that:

- SVs have an atomic clock, so the signal will be precisely sent at each interval. The time

Figure 3.2: The variation of the Doppler effect when receiver is acquiring authentic and spoofed signal. [3]



error on the positioning is based only on the receiver clock.

- satellites transmit at a constant power and are far away from the receiver. When the receiver moves, the satellites' power is constant on average. An attacker, however, needs to change their transmitting power according to the variation of the relative position between themselves and the victim.

- the autocorrelation function with the different signals is inconsistent, especially if the receiver is moving or if it implements a rotating antenna, in which case the spoofed signal's power received by the turning antenna increases and fades simultaneously, while authentic signal's power fades and increases according to the antenna position and the position of the satellite in space.

- Doppler effect can be considered for spoofing detection algorithms, as it is related to the relative movement between the orbiting satellites and the moving receiver. An example can be found in Figure 3.2

3.3 Integrity protection

The receiver, in order to be sure that the position it computed is the real one, needs some form of IP. In general, for both the open signal and the encrypted one, the transmission of the signal must guarantee a correct decoding of the data, i.e. the navigation message. To do so,

modulations and channel access must be chosen wisely. To provide a quick example, if simple modulations allow for a stronger signal, this also results in a lower symbol rate, requiring a longer time for an isolated receiver to be able to have its first fix, or first fixed position.

In the following two sections, I will go deeper with threats and countermeasures in place to maintain IP both at the data and signal levels.

3.3.1 IP at data level

For civilian use, the only GNSS system that provides IP at the data level is GALILEO commercial services. As was mentioned in chapter 2, GPS, GLONASS, and BeiDou offer IP for the military signals only. Without any integrity protection, the message sent to the signal can be spoofed just by sending around the wrong navigation message. As shown by [25], many mobile phones decode the satellite signal without even checking if the parameters sent are reasonable. By relating the results from [25] [25] with the discussion in [12], we can see that the problem needs to be addressed by all the systems, not only by GALILEO.

In order to guarantee IP, GALILEO commercial services include a message authentication and integrity protection mechanism similar to the Digital Signature Algorithm(DSA).

The name mechanism adopted by GALILEO to authenticate the navigation message, often referred as Navigation Message Authentication (NMA), is TESLA and works like in Figure 3.3. [26] First, a random key K_n is generated and a cryptographic hashing function is chosen. Then, the key K_n is hashed $n+1$ times obtaining K_0 the last derived key. This one is sent publicly at all devices and is called the root key. The first message to be sent, m_1, is then encrypted with K_1 and sent in the first time interval. After an amount of time, Δt, such that the transmitter can ensure that everyone has received the message, the transmitter publishes the key it used to encrypt m_1. After K_1 is published, the receiver proceeds as follows:

1. Verify that the key and the message were received with a delay equal to $\Delta t \pm \epsilon$. Then, check if the key arrived within the expected disclosure time. The receiver and the sender needs to have a synchronized clock with a negligible error with respect to the delay.

2. Verify that the key is a valid one, hashing it until it obtains the root key, K_0, or a number of times equal to n. If K_0 is not obtained, the key used to encrypt the message is considered not valid and the message is discarded. Otherwise, the receiver goes to the next step.

3. Using K_1, the receiver decrypts the received message and obtains m_1. Because the key was delayed and ensuring that the message arrived within limits, it accepts the data

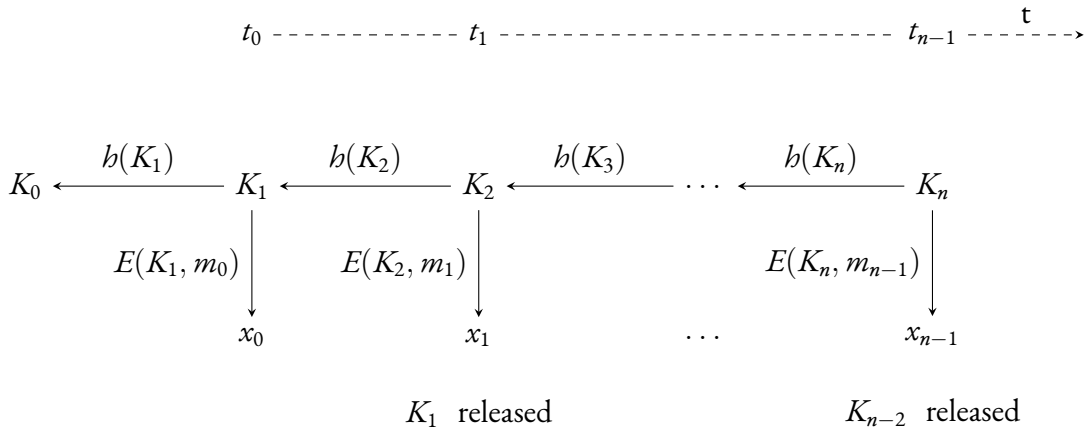


Figure 3.3: How TESLA protocol works. $h(\cdot)$ is the hashing function, $E(\cdot,\cdot)$ is the encryption function

contained in m_1

Each following message $(m_2, m_3, \ldots, m_n)$ is encrypted using $K_2, K_3, \ldots, K_n$ and the procedure described previously is repeated by the receiver.

The problem, then, is to store the root key safely and to have the possibility to access it only when it is in use. It has been proven, in fact [27], that the probability of successfully obtaining part of the keychain increases with time but also depends on the key length. This means that the keychain need to be changed periodically and that the root keys needs to be stored in each device. What it is needed, then, is a Key Management system.

Since the receiver does not have a lot of computational power, each root key is ciphered with a key that will be released as late as possible, but before the new keychain is used. Releasing the key as late as possible guarantees a small probability of success of obtaining part of the keychain using the pre-computation of the keychain that can generate K_0.

3.3.2 IP at signal level

At the signal layer, IP is given with techniques that analyze the channel behavior in relation with each signal. The military signal provided by GPS, GLONASS and BeiDou is authenticated using a long PRN code that is encrypted with an XOR operation with a secret key. This also provides IP to the NMA, but it does not add any IP at the signal level.

Measures to counteract spoofing by a generic receiver are well investigated and summarized[5], and are listed as follows.

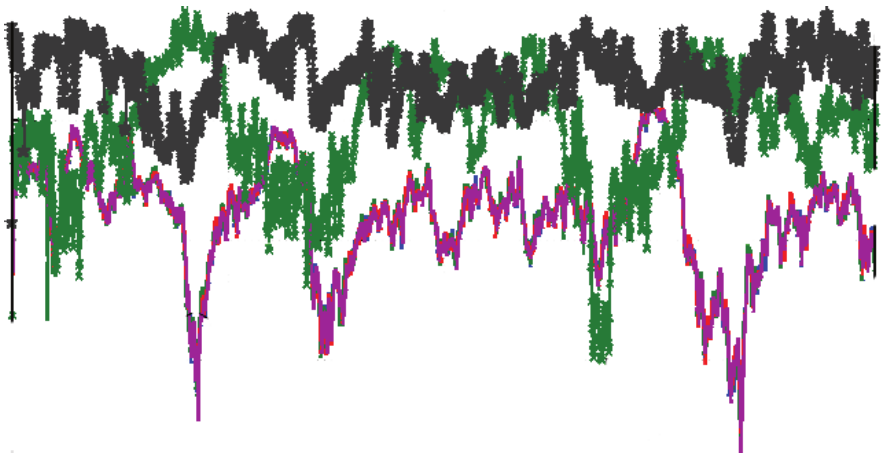


Figure 3.4: Correlation of amplitude with spoofed signal, as reported by [5]

- Measuring absolute power: the signal power at the receiver has an upper bound, which is given by the transmitting power at that frequency and the channel properties. In particular, the Automatic Gain Control (AGC) sets the LNA to correctly amplify the signal coming from the antenna(s). If the AGC is not monitored, it becomes source of vulnerability as it interfere with the signal power analysis done later.

- Signal power changes: authentic signals come from different satellites that are in different positions. This means that if the power of one satellite suddenly changes or the satellite powers become correlated, the receiver is under attack.

- Variation on SNR: a rapid change in SNR ($\frac{C_0}{N_0}$) either is due to a change in the receiver position (with a reduction of the ratio), or a spoofing attack beginning, and the SNR increasing.

- Correlation in signal behavior: if the different signal powers coming from different satellites at the receiver change with a high correlation, the signals of the different satellites are actually coming from one source, the attacker. This can be seen in Figure 3.4

- Rapid change in signal phase: the oscillators on the satellites are based on atomic clocks, so the phase change is almost null. On the other hand, a quartz oscillator has relevant changes on the oscillation period when compared to the one in the SV.

If the receiver has an Inertial Navigation System (INS), it can check if the movements registered via the satellite positions are coherent with the data coming from the INS device.

The following countermeasures, however, can only be performed if the receiver has an antenna array. In this list, I will specify if the countermeasure applies to only planar arrays or to both planar and linear arrays.

- Find the Angle of Arrival: with a linear array, the receiver can identify the angle from which the signal arrives along the line where the antennas are positioned. If the receiver has a planar array instead, it can identify the angle of arrival both in azimuth and direction.
- Ignore the spoofer: once a spoofer is identified using a particular phase shift of the incoming signal, the receiver can ignore the signal coming from that direction. This makes the attack unsuccessful.

The literature, though, has only analyzed the cases in which the attacker has only one antenna. An attacker with more antennas, though, could hypothetically deceive a multi-antenna victim by sending a signal that will be received as the legitimate satellite. This type of attack is the one I created for this thesis and I will discuss it further in the next chapter.

4

The attack

As shown in subsection 3.3.2, the possibility that an attacker could use more than one antenna to spoof their signal was never considered to the best of the author knowledge [24, 4, 3]. This allows a multiantenna receiver to defend itself easily, possibly by identifying the direction of the spoofed signal and rejecting by combining interference between the data coming from each element. The possibility to exploit the creation of spatial beams and the different analysis in the literature that focused on MIMO channels as channel matrices, allowed me to create this new type of attack.

4.1 The concept

Since the attacker has more than one antenna, they can create a beam that focuses the signal in a specific direction. This allows the spoofer to concentrate all the power in one lobe (whose size depends on the number of antennas) and hit only one target. This can be done with a phased square array. The two parameters to direct the signal are two angles. One of the two is the elevation to respect of the plane of the array; the other is the angle created projecting the vector that connects the transmitter to the receiver on the surface of the planar array and the direction over one axis, that is the direction of the vector of 0°. If multiple stations are receiving the GNSS signal and the attacker wants only one of the possible victims to be affected, they can exploit the possibility to generate a beam hitting only the intended receiver. More than this, the attacker can exploit the fact that MIMO channels can be considered as

matrices that link the transmitting antennas to the receiving ones. In particular, a spoofer that has more antennas than the receiver sees the MIMO channel as

$$\overrightarrow{RX} = \mathrm{H} \cdot \overrightarrow{TX} \tag{4.1}$$

where

- $\overrightarrow{RX} \in \mathbb{C}^N$ is the vector of the receiving antennas. The number of elements at the receiver is N;
- $\mathrm{H} \in \mathbb{C}^{N \times M}$ is the channel matrix;
- $\overrightarrow{TX} \in \mathbb{C}^M$ is the transmitting vector which has M elements.

Both the matrix and the two vectors are complex, as they represent the signals transmitted by that device. If $M \geq N$, that is, the spoofer has more antennas than the receiver, the channel matrix can be pseudo-inverted and we can have:

$$\overrightarrow{TX} = \mathrm{H}^{\dagger} \cdot \overrightarrow{RX} \tag{4.2}$$

where the † stands for the pseudo inverse operation.

With this knowledge, the spoofer can create the signals that each antenna at the receiver must see, and knowing the channel conditions at its side, the results of Equation 4.2 lead to the signals to transmit. The attacker, then, needs to know the position of the satellites in order to generate signals such that the received data appears to come from a specific direction.

Now that the receiver has the signals to send, it generates the phase differences so that the waves going out from the array elements will interfere and the beam will go only in the direction of the victim.

4.1.1 Physical devices involved in the attack

For this type of attack, the spoofer needs a planar antenna array, a distance measuring tool, a GNSS receiver to estimate the actual channel conditions, and a computer to process data. Planar arrays can have different shapes, but they must be known to correctly compute the correlation matrix at the transmitter. The distance measuring tool is used to see the distance between the spoofer and the receiver so that the spoofer can adjust the transmitted power in order to avoid the receiver detecting an abnormally high power level and Signal-to-Noise

Ratio (SNR). The computer needs to be powerful enough to be able to track the receiver's position and velocity such that it can modify the transmitted signal coherently with what the receiver is doing, i.e. to apply a doppler shift if the receiver is moving or change the signal power if the victim is moving in a particular direction that loses the LoS with the satellite.

4.1.2 Algorithm

In the following I will explain how the attack works in its details, in order to be able to succeed. The two letters A and V will be used to define the attacker and the victim respectively.

1. A becomes aware of its relative position to V, and if possible, the relative and absolute speed
2. A becomes aware of V antenna array position. If not, the receiver assumes that the antenna is on the roof of the vehicle
3. A begins to gradually interfere with the signal, so that V experiences a lowering in SNR.
4. A knows how many antennas the victim has and their inter-distance
5. A computes the arrays correlation matrices at its side and at V's side
6. A computes the Doppler shift of the signal that it aims to transmit to V according to the real SVs's position and A's relative speed
7. Knowing the following, A creates the signals that each antenna at V needs to receive
    - The legitimate DoA knowing V and the SV positions
    - The number of antennas that V has
    - The array antenna distance on V's side
8. A samples the channel conditions, and, knowing the correlation matrices, computes the signal that it needs to transmit so that each antenna on V's side will be tricked into processing the spoofed DoA. A inverts the channel matrix, so that the receiver will receive the signal the attacker wants it to get. The proof is in section 4.2
9. A generates the waves they need to transmit in order for the signals to reach V's position alone, and these signals are sent.
10. A iterates from step 6 to step 9 as necessary.

4.2 Mathematical proofs

An attacker that knows the channel perfectly, will prepare the signal so that each receiver antenna will receive the spoofed signal decided on by the attacker. There are two families of channels: the LoS channel, which uses a Rician model, and the Non-Line of Sight (NLoS) channel, which uses a Rayleigh model. The MIMO channel equations are:

$$\begin{aligned} H &= \sqrt{\frac{k}{k+1}} \cdot H_0 + \sqrt{\frac{1}{k+1}} \cdot R_R^{\frac{1}{2}} \cdot H_w \cdot R_T^{\frac{1}{2}} \quad \text{for a Rician channel} \\ H &= R_R^{\frac{1}{2}} \cdot H_w \cdot R_T^{\frac{1}{2}} \qquad\qquad \text{for a Rayleigh channel} \end{aligned} \tag{4.3}$$

Since both the authentic signal and the real signal come from a LoS channel, I used the Rician channel model with a fixed value for K.

If the attacker knows the channel perfectly, the procedure they will follow is:

1. Invert the channel matrix H $\implies$ $H^{-1} = pinv(R_R^{\frac{1}{2}} \cdot H_w \cdot R_T^{\frac{1}{2}})$, with $pinv(\cdot)$ the Moore-Penrose right pseudoinverse of a matrix. If H is N_R-by-N_T, with $N_T > N_R$, the pseudoinverse is always possible.

2. Multiply the signal $s \in \mathbb{C}^{N_R \times l_s}$ by H^{-1} and obtaining $x = H^{-1} \cdot s$. $x \in \mathbb{C}^{N_T \times l_s}$, with l_s being the length of the signal in number of samples.

3. the receiver will get a signal $r = H \cdot x = H \cdot H^{-1} \cdot s = s$. So the receiver will get the signal the attacker wants.

To transmit in a specific direction, the literature shows[28] that the beam can be steered using the array factor AF. In general, to steer the beam to an azimuth angle ϕ and an elevation angle θ, we need to transmit:

$$X_{m,n} = \sum_{m=1}^{TX_x} \sum_{m=1}^{TX_y} I_0 \cdot \exp^{\jmath\, \beta(m-1)d_x \sin(\theta)\cos(\phi) + \jmath\, \beta(n-1)d_y \sin(\theta)\cos(\phi)} \tag{4.4}$$

where

- $m = 1, n = 1$ the reference antenna
- $I_0 \in \mathbb{C}$ the complex signal to be transmitted
- $\beta = \frac{2\pi}{\lambda}$, the wave number

- d_x and d_y as the inter-element distance
- TX_x the number of antennas along the x axis
- TX_y the number of antennas along the y axis

4.3 Simulations and results

The simulations were done in MatLab with one and two signals arriving from different directions. The simulator asks for:

- the number of antennas at transmitter and receiver antenna arrays
- the distance between the elements of the arrays
- the direction of arrival of each signal
- the signals to be transmitted
- the position of the attacker and the receiver in 3 dimensions
- the signal frequencies

The first operation on the single signal is to convert it to N signals, applying the transformation in Equation 4.4. The output will be a 3D matrix ($N_{RX,1} \times N_{RX,1} \times l_s$) that will be transformed into a 2D matrix ($(N_{RX,1} \cdot N_{RX,1}) \times l_s$). This will be the array of signals the receiver will get.

Then, from the number of antennas and their relative positions, the attacker calculates the spatial correlation matrices. As reported in literature, the usual channel matrix can be computed as shown in the Mathematical proofs section.[29, 30]

After this step, the signal s will be multiplied by the inverse of the channel, obtaining x. If a signal like this were to be sent and received, it is obvious the attack would always be successful. In this thesis, I tested how much the attacker needs to know about the channel. In particular, given H_a (the attacker channel from Equation 4.3), I generated an independent channel H_u, which represents the unknown channel with a different Gaussian normal matrix H_w, named H'_w. From this process I generated:

$$H_a = \sqrt{\frac{k}{k+1}} \cdot H_0 + \sqrt{\frac{1}{k+1}} \cdot R_R^{\frac{1}{2}} \cdot H_w \cdot R_T^{\frac{1}{2}} H_u = \sqrt{\frac{k}{k+1}} \cdot H_0 + \sqrt{\frac{1}{k+1}} \cdot R_R^{\frac{1}{2}} \cdot H'_w \cdot R_T^{\frac{1}{2}} \quad (4.5)$$

and I generated a channel which is

$$\hat{H} = \rho \cdot H_a + (1 - \rho) H_u \quad (4.6)$$

When $\rho \approx 0$, the attacker knows little about the real channel $\hat{H}$. Instead, when $\rho \approx 1$, the attacker knows the channel almost perfectly. In particular $\rho = 0$ means that there is absolutely no knowledge about the channel, and $\rho = 1$ means that the channel the attacker used is the same as the real channel.

Then, I simulated the signal $r = \hat{H} \cdot x$ being received and using the Multiple Signal Classification (MuSiC) algorithm, I let the receiver find from which direction the signal originated. I took the error between the DoA wanted by the attacker and the DoA measured by the receiver as the performance measure. Table 4.1 shows the average error where

- one signal was transmitted
- the azimuth was varied between $-170°$ and $180°$ with a step of $10°$
- the elevation was varied between $-80°$ and $10°$ with a step of $10°$

The outliers I experienced are shown in Figure 4.1, and they were randomly placed in the range $[0.92; 0.988]$. Since the spikes occured only for one value and were not present in every combination, the reason for this is believed to be caused by a sampling error. In the range $[0.7; 1]$ the step between two adjacent ρ was set as 0.002, so this reason could be believed to be true.

In Figure 4.3 it is represented the error on the estimation, when two signals coming from different DoAs were hitting the receiver with the same power. The two average errors are listed in Table 4.2 and shown in a plot in Figure 4.3. As the reader can see, the error between the estimated and the spoofed angle is higher than the single signal case. Because of this, if the attacker does not know the channel better than the case before, the receiver will be able to find where the spoofer is.

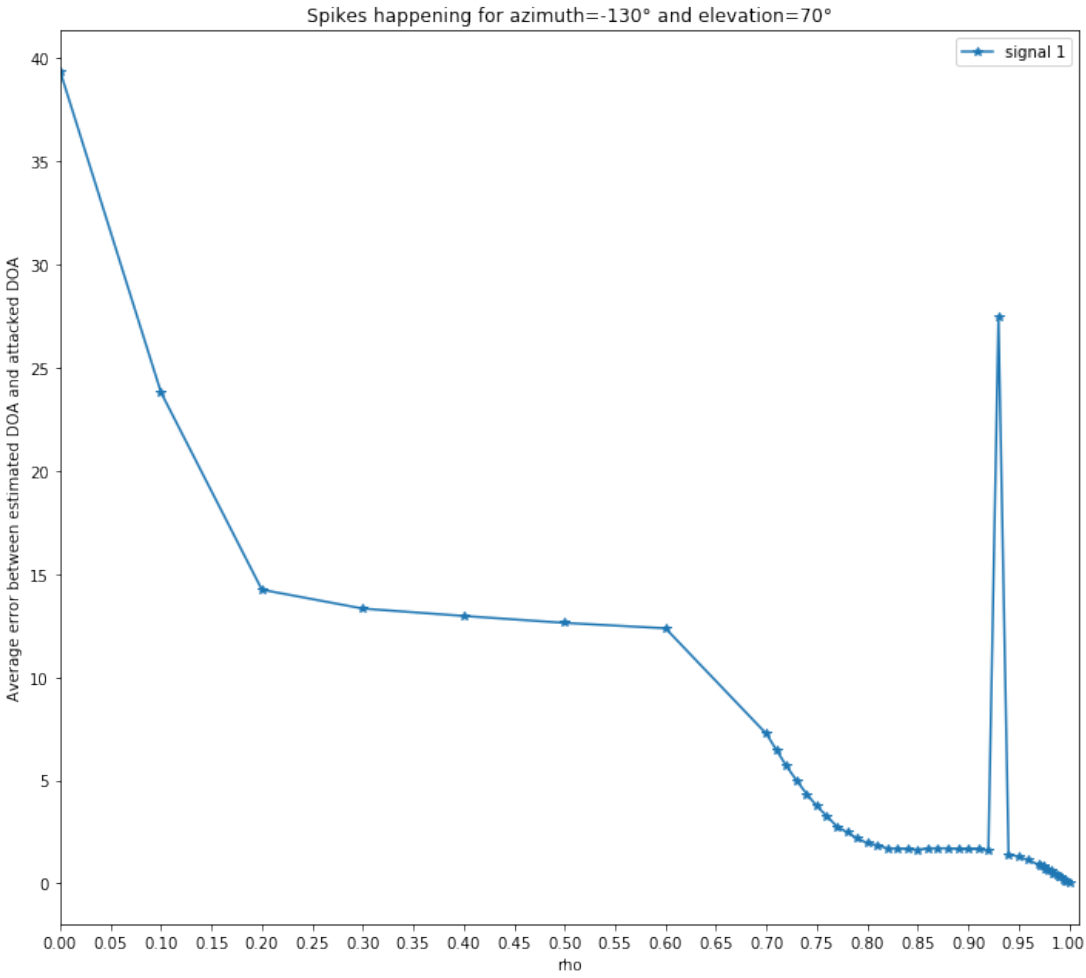


Figure 4.1: The spike that can be found when analyzing the computed DoA

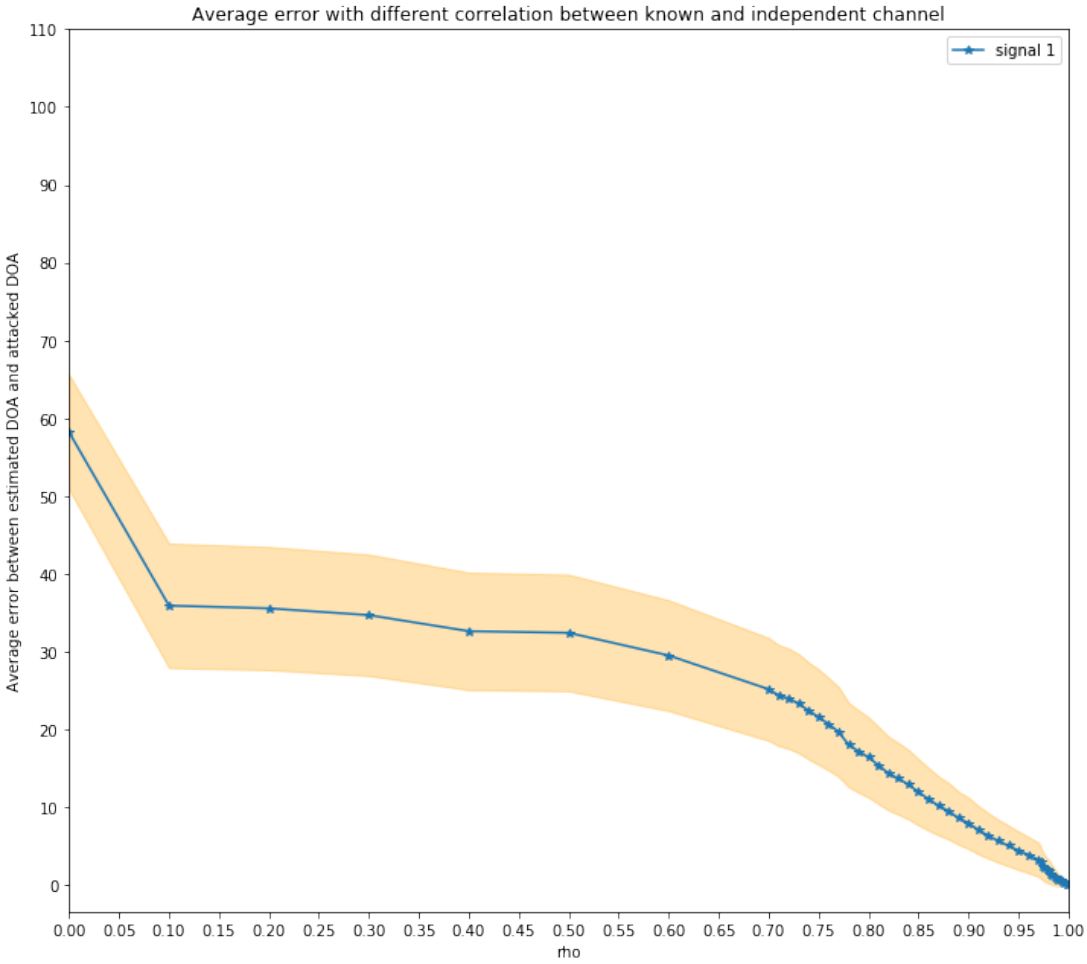


Figure 4.2: The average error when varying the correlation value and without the spikes. Values can be found in Table 4.1. The lighter color represents the standard deviation.

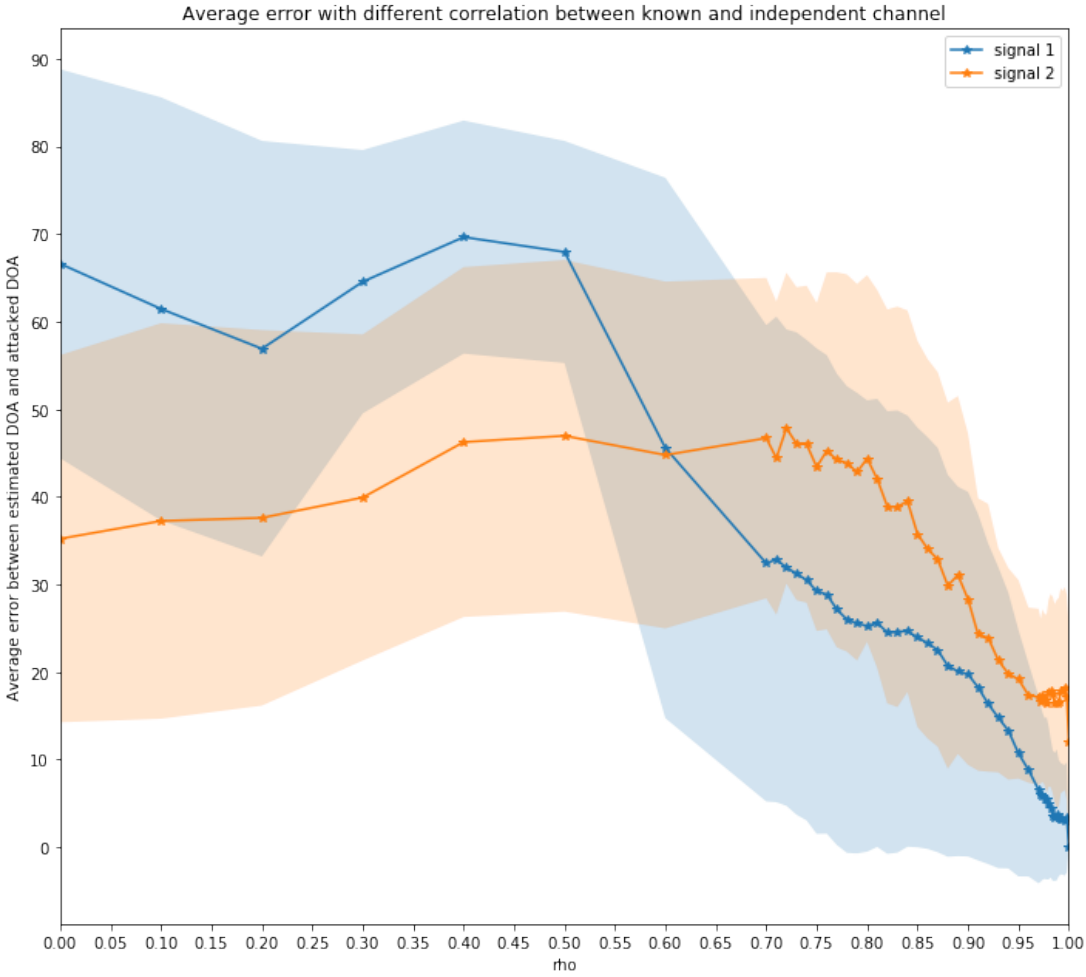


Figure 4.3: Average absolute error between the DoAs chosen by the attacker and the DoAs estimated by the receiver of the two signals transmitted. The lighter color represents the standard deviation.

ρ	error	ρ	error
0.0	66.6100	0.88	20.7141
0.1	61.4574	0.89	20.0778
0.2	56.9145	0.9	19.7600
0.3	64.5614	0.91	18.2601
0.4	69.6526	0.92	16.3777
0.5	67.9568	0.93	14.8038
0.6	45.5814	0.94	13.3213
0.7	32.4176	0.95	10.7403
0.71	32.8637	0.96	8.8286
0.72	31.9237	0.97	6.5689
0.73	31.2529	0.972	6.0919
0.74	30.4901	0.974	5.8171
0.75	29.2431	0.976	5.5684
0.76	28.8682	0.978	5.5819
0.77	27.1571	0.98	5.0441
0.78	25.9961	0.982	4.4343
0.79	25.5886	0.984	3.6336
0.8	25.2572	0.986	3.4567
0.81	25.6174	0.988	3.6973
0.82	24.5175	0.99	3.3306
0.83	24.6241	0.992	3.2618
0.84	24.6721	0.994	3.1701
0.85	23.9493	0.996	3.0820
0.86	23.3121	0.998	3.4350
0.87	22.5106	1.0	0.0000

Table 4.1: Average absolute error between the DoA chosen by the attacker and the DoA estimated by the receiver.

ρ	error signal 1	error signal 2	ρ	error signal 1	error signal 2
0.0	66.6100	35.2220	0.88	20.7141	29.8615
0.1	61.4574	37.2512	0.89	20.0778	31.0876
0.2	56.9145	37.6085	0.9	19.7600	28.3295
0.3	64.5614	39.9334	0.91	18.2601	24.2967
0.4	69.6526	46.2554	0.92	16.3777	23.9123
0.5	67.9568	46.9723	0.93	14.8038	21.3617
0.6	45.5814	44.7779	0.94	13.3213	19.8016
0.7	32.4176	46.7082	0.95	10.7403	19.1788
0.71	32.8637	44.4291	0.96	8.8286	17.3672
0.72	31.9237	47.8444	0.97	6.5689	17.1598
0.73	31.2529	46.0739	0.972	6.0919	16.6913
0.74	30.4901	46.0082	0.974	5.8171	17.3091
0.75	29.2431	43.4141	0.976	5.5684	16.8557
0.76	28.8682	45.2591	0.978	5.5819	16.3952
0.77	27.1571	44.2281	0.98	5.0441	17.6068
0.78	25.9961	43.8640	0.982	4.4343	17.8900
0.79	25.5886	42.8118	0.984	3.6336	17.4216
0.8	25.2572	44.3795	0.986	3.4567	16.4231
0.81	25.6174	42.0437	0.988	3.6973	16.3675
0.82	24.5175	38.9126	0.99	3.3306	16.5433
0.83	24.6241	38.8632	0.992	3.2618	17.8615
0.84	24.6721	39.5042	0.994	3.1701	17.8164
0.85	23.9493	35.7472	0.996	3.0820	14.1144
0.86	23.3121	34.0706	0.998	3.4350	8.1379
0.87	22.5106	32.8588	1.0	0.0000	0.0000

Table 4.2: Average absolute errors between the DoAs chosen by the attacker and the two DoAs estimated by the receiver.

5 Conclusion

As GNSS systems are becoming more and more ubiquitous, it is necessary to guarantee users the reliability of the position they are obtaining. Civilian signals are becoming ever more widely used by hundred of millions people worldwide, but even more important than these applications are commercial services, which need to guarantee an even greater trustworthiness to receivers used in agriculture, aviation, ATMs, and so on.

Many steps have been taken to achieve IP both at the signal level and at the data level, which ensures the reliability of the received signal. Attackers, however, are always trying to find new ways to control their victims. This thesis aimed to discover a novel spoofing attack technique and demonstrated that an attacker could send a particular signal from multiple antennas so that the receiver is unaware of being spoofed and will trust a fake signal coming from a different direction than the authentic one. The success rate I achieved when the attacker knows the channel correctly should encourage future research to address this possible problem and possibly find some similar attacks that were not investigated in this work. In the next section, I will suggest some possible future works that may be done.

5.1 Future Works

As this thesis is merely analytical, one suggestion would be to create a prototype to determine when this type of attack could work in the real life and the capabilities that could be achieved with tracking algorithms. The limitations of this attack should also be analyzed, so that the

receiver may implement algorithms to exploit them.

Another variation of this attack (that could be impractible as the number of antennas required by an attacker is quite high) could be the generation of N beams, one per receiving antenna element. This allows the attacker to send each antenna its own particular signal, in order to better ensure that the receiver is spoofed. A problem with this attack, though, is that it needs the attacker to accurately hit the antenna element, roughly 20cm by 20cm, from a far distance. The Beam Width First Null, meaning the aperture of the beam at the main lobe generated by the attacker array, must be really tight.

A possible defense to my attack, as shown by the literature, (but with different condition) could be checking if a receiver is under attack by using one antenna that is rotating on its axis at a random speed. With this trick, the attacker is not able to correctly modulate the power of each signal and mask itself. The receiver, then, could easily find the direction of the attack by maximizing the spoofed signal's power it is experiencing.

Acknowledgments

My gratitude could start only with my advisor Prof. Nicola Laurenti and my co-advisor M.Sc. Silvia Ceccato of the Department of Information Engineering at the University of Padua, without whom this thesis could not be possible.

Then, my thanks go to both my Mom and Dad for having had my back over all these years and being there to share all the joyful moments and the harder ones that have happened in my life.

Then, for sure I cannot thank enough and in equal measure all my grandparents that helped my parents to raise me to be the person I am today. A huge thanks also, goes to all my relatives for indulging all my curiosity and allowing me to look at the new objects, topics, and ideas with the astonishment I carry with me today.

Last but not least, I want to thank all my friends, offline and online, for sharing with me all the happy, stressed out, and hard moments. Without them, I would not be where I am.

References

[1] J. S Warner and R. G Johnston, "GPS spoofing countermeasures," vol. 25, p. 8, 01 2003.

[2] Z. Haider and S. Khalid, "Survey on effective GPS spoofing countermeasures," in 2016 Sixth International Conference on Innovative Computing Technology (INTECH), Aug 2016, pp. 573–577.

[3] A. Broumandan, A. Jafarnia-Jahromi, S. Daneshmand, and G. Lachapelle, "Overview of spatial processing approaches for GNSS structural interference detection and mitigation," Proceedings of the IEEE, vol. 104, no. 6, pp. 1246–1257, June 2016.

[4] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," Proceedings of the IEEE, vol. 104, no. 6, pp. 1258–1270, June 2016.

[5] J. N. Ali Jafarnia-Jahromi, Ali Broumandan and G. Lachapelle, "GPS vulnerability to spoofing threats and a review of antispoofing techniques," International Journal of Navigation and Observation, vol. 2012, no. 127072, p. 16, 2012.

[6] N. Vagle, A. Broumandan, and G. Lachapelle, "Analysis of multi-antenna GNSS receiver performance under jamming attacks," Sensors, vol. 16, p. 1937, 11 2016.

[7] J. Magiera and R. Katulski, "Detection and mitigation of GPS spoofing based on antenna array processing," Journal of Applied Research and Technology, vol. 13, no. 1, pp. 45 – 57, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1665642315300043

[8] J. Arribas, C. Fernández-Prades, and P. Closas, "Multi-antenna techniques for interference mitigation in GNSS signal acquisition," EURASIP Journal on Advances in Signal Processing, vol. 2013, no. 1, p. 143, Sep 2013. [Online]. Available: https://doi.org/10.1186/1687-6180-2013-143

[9] D. Marnach, S. Mauw, M. Martins, and C. Harpes, "Detecting meaconing attacks by analysing the clock bias of GNSS receivers," Artificial Satellites, vol. 48, p. 19, 01 2013.

[10] Satellite navigation - GPS - presidential policy. [Online]. Available: https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/gnss/gps/policy/presidential/

[11] New civil signals. [Online]. Available: https://www.gps.gov/systems/gps/modernization/civilsignals/

[12] C. Hwong. Verto index: Travel. [Online]. Available: https://www.vertoanalytics.com/verto-index-travel/

[13] DSP-CS-6, Navstar Global Positioning System (GPS). [Online]. Available: https://quicksearch.dla.mil/qsDocDetails.aspx?ident_number=216352

[14] T. Mai. Global positioning system history. [Online]. Available: https://www.nasa.gov/directorates/heo/scan/communications/policy/GPS_History.html

[15] P. Higbie and N. Blocker, "The nuclear detonation detection system on the gps satellites."

[16] Glonass history. [Online]. Available: https://glonass-iac.ru/en/guide/index.php

[17] P. Closas and A. Gusi-Amigo, "Direct position estimation of GNSS receivers: Analyzing main results, architectures, enhancements, and challenges," IEEE Signal Processing Magazine, vol. 34, no. 5, pp. 72–84, Sep. 2017.

[18] M. Szabova and F. Duchon, "Survey of GNSS coordinates systems," European Scientific Journal, ESJ, vol. 12, no. 24, p. 33, 2016.

[19] B. C. Barker, J. Betz, J. E. Clark, J. T. Correia, J. Gillis, S. Lazar, K. A. Rehborn, and J. R. S. , III, "Overview of the GPS m code signal," p. 9, 01 2006.

[20] G. R. Lennen, "The ussr's glonass p-code - determination and initial results," pp. 77 – 83, 01 1989.

[21] I. Fernandez-Hernandez, J. Simón, R. Blasi, C. Payne, T. Miquel, and J. P Boyero, "The Galileo commercial service: Current status and prospects," 04 2014.

[22] Galileo: Secure satellite navigation for emergency and security services. [Online]. Available: http://europa.eu/rapid/press-release_IP-10-1301_en.htm

[23] B. Zhao and S. Zhang, "Rethinking spatial data quality: Pokémon go as a case study of location spoofing," The Professional Geographer, vol. 71, no. 1, pp. 96–108, 2019. [Online]. Available: https://doi.org/10.1080/00330124.2018.1479973

[24] P. Papadimitratos and A. Jovanovic, "GNSS-based positioning: Attacks and countermeasures," in MILCOM 2008 - 2008 IEEE Military Communications Conference, Nov 2008, pp. 1–7.

[25] S. Ceccato, F. Formaggio, G. Caparra, N. Laurenti, and S. Tomasin, "Exploiting side-information for resilient GNSS positioning in mobile phones," in 2018 IEEE/ION Position, Location and Navigation Symposium (PLANS), April 2018, pp. 1515–1524.

[26] S. Binda. (2018, 01) Galileo open service navigation message. GNSS Interferentie en Authenticatie, Haarlem, NL. European Space Agency. [Online]. Available: http://www.navnin.nl/new/wp-content/uploads/2018/02/WSIA-4-ESA-NIN-Workshop-Galileo-NMA.pdf

[27] A. Neish, T. Walter, and P. Enge, "Parameter selection for the TESLA keychain," vol. 31st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2018), 09 2018, pp. 2155–2171.

[28] O. Manu, M. Dimian, and A. Graur, "Analysis of beamforming in phased antenna arrays," Development and Application Systems, p. 79, 2010.

[29] L. Zhang and X. Wang, "On the precoder design for mimo systems over correlated rician channels," in 2013 IEEE 78th Vehicular Technology Conference (VTC Fall), Sep. 2013, pp. 1–5.

[30] A. A. Kalachikov and N. S. Shelkunov, "Construction and validation of analytical wireless mimo channel models based on channel measurement data," in 2018 XIV International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE), Oct 2018, pp. 175–179.

[31] A. Schmid, A. Neubauer, H. Ehm, R. Weigel, N. Lemke, G. Heinrichs, J. Winkel, J. A. Ávila Rodríguez, R. Kaniuth, T. Pany, B. Eissfeller, G. Rohmer, and M. Overbeck, "Combined Galileo/GPS architecture for enhanced sensitivity reception," AEU - International Journal of Electronics and Communications, vol. 59, no. 5, pp. 297 – 306, 2005. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1434841105000877

[32] C. Wullems, O. Pozzobon, and K. Kubik, "Signal authentication and integrity schemes for next generation global navigation satellite systems," in European Navigation Conference (ENC-GNSS 2005), Munich, Germany, July 2005. [Online]. Available: https://eprints.qut.edu.au/38275/

[33] P. Papadimitratos and A. Jovanovic, "Protection and fundamental vulnerability of GNSS," in 2008 IEEE International Workshop on Satellite and Space Communications, Oct 2008, pp. 167–171.

[34] V. Oehler, F. Luongo, H. L. Trautenberg, J.-P. Boyero, J. Krueger, and T. Rang, "The Galileo integrity concept and performance," 2005, p. 11.

[35] O. Pozzobon, C. Wullems, and K. Kubik, "Secure tracking using trusted GNSS receivers and Galileo authentication services," Journal of Global Positioning Systems, vol. 3, no. 1-2, pp. 200–207, 2004. [Online]. Available: https://eprints.qut.edu.au/38282/

[36] J.-H. Lee and C.-C. Cheng, "Spatial correlation of multiple antenna arrays in wireless communication systems," Progress In Electromagnetics Research, vol. 132, p. 22, 01 2012.

[37] H. Gazzah and S. Marcos, "Cramer-rao bounds for antenna array design," IEEE Transactions on Signal Processing, vol. 54, no. 1, pp. 336–345, Jan 2006.

[38] O. A. Oumar, M. F. Siyau, and T. P. Sattar, "Comparison between MUSIC and ESPRIT direction of arrival estimation algorithms for wireless communication systems," in The First International Conference on Future Generation Communication Technologies, Dec 2012, pp. 99–103.

[39] A. Lehner and A. Steingaß, "A novel channel model for land mobile satellite navigation," 01 2005, p. 7.

[40] P. Y Montgomery, T. E Humphreys, and B. M. Ledvina, "Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer," Proceedings of the Institute of Navigation, National Technical Meeting, vol. 1, pp. 124–130, 01 2009.

[41] A. Broumandan and G. Lachapelle, "Spoofing detection using gnss/ins/odometer coupling for vehicular navigation," Sensors, vol. 18, p. 1305, 04 2018.

[42] W. Xiong, Z. Mo, G. Chen, H. Liu, K. Pham, and E. Blasch, "Distributed coherent mimo system with advanced cdma channel estimation," in 2017 IEEE Aerospace Conference, March 2017, pp. 1–7.

[43] J. Shi and M. Ho, "Mimo broadcast channels with channel estimation."

[44] A. Abdi, C. Tepedelenlioglu, M. Kaveh, and G. Giannakis, "On the estimation of the k parameter for the rice fading distribution," IEEE Communications Letters, vol. 5, no. 3, pp. 92–94, March 2001.

[45] W. Y. Ochieng, K. Sauer, D. Walsh, G. Brodin, S. Griffin, and M. Denney, "Gps integrity and potential impact on aviation safety," Journal of Navigation, vol. 56, no. 1, p. 51–65, 2003.